SUMMARY OF INSIGHTS

July 23, 2010

"Turnkey" Approach to Statewide Data Center
Request for Information A10-RFI-055

EXECUTIVE SUMMARY OF RESPONSES

(1) There is significant vendor interest in participating in the private cloud aspect of the data center.

(2) Some vendors have explicitly mentioned interest in helping to attract tenants to the data halls that do not have planned occupancy at this time.

(3) Several potential bidders on a future RFP have business units that build private clouds for customers along the lines of the effort we imagine for the state.

(4) Some of the vendors have expressed willingness to financially support the initial efforts. This will require extensive legal review, dialogue with the Treasurer, and other groundwork.

(5) The technical boundaries of a potential RFP may expand. The data center combines mainframe systems, servers with individual applications, and the private cloud servers and applications. Many vendors recommend expanding the scope well beyond the cloud computing component to include storage, disaster recovery, network and – perhaps – mainframes and telephony. Questions remain about whether and how these might be incorporated in an RFP.

(6) The RFI specifically asked vendors about training state employees and handing the facility back to public operation in the future. Responses accepted this premise. The financial model and specifics of this staffing model will need to be addressed in any future RFP.

(7) Most responses devoted considerable effort to describing the transition and governance issues involved in moving toward a shared state data center. There is a clear message that transition costs will exceed hardware and software cost.

(8) Any resulting RFP will need to address the intersection of existing governance strategies and bodies and the vendor effort.

(9) The Review Team members feel strongly that it would be beneficial to schedule follow up conversations with some of the respondents.

DESCRIPTION OF THE REQUEST FOR INFORMATION

On May 27, 2010, Washington issued a Request for Information ("RFI") for strategic advice, equipment, initial operation, and transition training related to the shared and virtualized portions of a 60,000 square foot statewide data center. This RFI was to explore the potential for a "turnkey" approach to the private cloud inside the new statewide data center. The goal was to gain insight into the potential for a vendor to finance, provision and launch the effort, provide training to state employees, and transition the ownership and operation of the facility to the state. Responses were due on July 2, 2010. 15 responses were received.

Washington's information technology strategy is transforming from a largely distributed operating environment to a largely consolidated environment. This will be achieved through a combination of strategies that includes server virtualization, capacity on demand, managed storage networks, statewide sharing of common tools, and implementation of "virtual containers" in which agencies exercise a degree of autonomy and isolation in managing their portion of the state's private cloud. Balancing computing, networking, and security will need to be a central feature of any solution. Virtualization of desktops is also a topic of discussion. Shared services and their attendant implied change of funding model is also driving the discussion. To enable the Department of Information Services to focus on continuing to deliver services (including a physical ala carte environment) during the transition to a new operating environment, the Department is seeking a partner with the intention that a phased change of responsibilities from the partner's staff to the State's will occur through intensive training in the operating principles of the new environment. Toward that end, the Department is developing information about the potential for a vendor to establish and operate a statewide data center while working side-by-side with state employees who are being trained to operate the completed data center. The relevant portions of the new facility are those providing the private cloud for the public sector within the facility. In the RFI context, vendors were told to assume the mainframe equipment and legacy applications were not in the mix of services and equipment under discussion. The focus was primarily on the virtualized operating environment providing common services.

The timing and specifics of this approach were left open for purposes of this RFI because a vendor may propose a timeline that corresponds to a preferred leasing arrangement, ownership structure, or financing model. Given the intense fiscal pressures on the state, the Department is particularly interested in approaches that reflect creative, lower cost financing and billing of agencies. Given the potential for a broad range of public institutions (higher education, other levels of government, etc.) utilizing this facility in the future, the Department is also interested approaches that would permit these collaborations in the future.

ORGANIZATION OF THIS REPORT

This report is the result of extensive review of the responses to the RFI. DIS assigned three teams: financial, legal/contracting, and operations. In addition to the formal review process, Chief Information Officers from agencies and other individuals have reviewed the results and offered comments. Because this is a Request for Information and not a Request for Proposals, the outcome of the effort is a summary of insights, not a ranking of potential bidders. Indeed, the eventual outcome is likely to be a Request for Proposals that reflects many insights from many of the responses.

This report has two broad sections:

(1) Summaries of responses to the nine questions in the RFI. Some questions where within the scope of a given review team and some were not. The report shows which review team provided a summary for a particular question. The discussion of each question concludes with insights about future contracting that are specific to the question under discussion.

(2) Summaries of insights from the three DIS review teams reflecting important lessons for any future contracting around a turnkey data center operation. These are insights that were gained from the review process that were broader than any specific question in the RFI. These are organized by review team.

RESPONSES TO SPECIFIC QUESTIONS

1. What are the financial, legal, and operational advantages and disadvantages of the model under investigation relative to a fully state run transition and operation? Are there unique telephony issues about which we should be aware?

Operational Review:

- Multiple conceptual alternatives were described, ranging from standing up solution and turning over to the state or running on behalf of the state or moving the solution to the vendor site.
- Most vendors recommended a separate engagement to perform an assessment and did not provide a technical approach. Recommendation to conduct an infrastructure assessment to gather requirements, assess operational readiness, assess business objectives, develop a strategic implementation plan, implement plan over time with identifiable wins, communicate your success internally, metrics, volume and speed.
- Vendors are looking for assessment on assets, compliance requirements, security requirements
- Issues surfaced by respondents about telephony tie back to network and design.

- Responses fell into three categories: One sells Project Management with no product to sell and they will provide best practices, some have products to sell, and the remainder were integrators that bring all together to implement.
- Mix of responses on monitoring and management of tool sets. Some have a mix of monitoring and management between vendor and state while other proposed vendor-only solution.
- Several different approaches on staffing. Approaches ranged from having state staff assist in the implementation using state resources up front. Other approaches had vendor provide 2 on 1 training at time of transition from vendor to the state.
- None of responses provide a definite number of employees required to support the system after implementation and transition back to the state.
- Multiple responses recommend leveraging a portal to enable On-Demand self-service for users including information on “pay as you use” (consumption-based charge back model) using low touch on the back end infrastructure (automation).
- Responses are very light regarding overall service desk support and responses to users.
- Several advantages include: vendor assistance in skill assessment, vendor setup of a turnkey solution minimizing impact on daily operation while solution is being established, reduced FTE cost, reduced physical infrastructure, and vendor capital availability.
- Several disadvantages include: significant commitment to single vendor, vendor will have learning curve on agency specific needs, agency loss of managerial control, and cultural shift.

Financial Review:

- Legal advantage: DIS can sell to non-profit corporations and local governments.
- Several vendors mentioned the ability to transform CAPEX to OPEX and the potential to lower both.
- Increased utilization/efficiencies are a common goal among the respondents.
- Opportunities about to simplify support of infrastructure through smart design.
- Stipulations in funding sources may restrict use of funds.

Inputs for acquisition:

- Provide “as is” information gathered from agencies in the Shared Services work as well as the TPI, PTI and Excipio studies.
- Make available information on state networking infrastructure (IGN, PGN, ISB standards).
- Determine how we would ask vendor questions on speed, feeds, and length of time.
- When issuing an RFP, the state needs to be clear about what we are buying and describing for telephony, storage, disaster recovery, network and (if applicable) mainframes. The vendors provided many different interpretations of telephony.

- Include detailed glossary of terms (different definition for pods, containers, disaster recovery, etc.)
- For an RFP, a decision should be made about what the state intends in terms of architecture. Will we be asking the vendor to support open standards or is proprietary acceptable approach?
- Will need to develop exit strategy to migrate from one architecture to another. Have the vendor provide information on an exit strategy to accommodate changing technology so the state can evaluate the ability to change.
- Support strategy to leverage existing investment in infrastructure.
- Vendor to identify shared tool set for managing and monitoring solution set. Include information on ability to minimize management tool solutions.
- For an RFP, recommend leveraging information on the eBay training model as a guideline to establish accountability initially with the vendor and transition to the state employee.
- Need to ask the vendor about the roles, responsibilities, and number of employees needed for implementation, time requirements, and on-going maintenance. This will enable the state to assess the future cost implications.
- Determine as a state how we want to procure a solution. Metered consumption chargeback model, fixed rate model, or other cost recovery model. This will determine how much risk will be split between the state and the vendor.
- Outline information on integrating Service Desk component between vendor and the state.

2. How would this deployment strategy address unique aspects of the centralized state data center such as security concerns and disaster recovery? For background on state standards, see the Information Services Board: http://isb.wa.gov/policies/Default.aspx

Operational Review:

- Vast gap in the vendor responses related to security and Disaster Recovery (DR).
- Some vendor provided details on ability to meet most but not all of security/regulatory requirements that the state must comply with such as IRS and FERPA.
- A few responses mentioned an additional fee to include a DR solution.

Inputs for acquisition:

- Need to include information on how the solution will integrate with the state security gateways.
- Need to include information on approach to authentication leveraging existing state security solutions.
- Need to articulate in an RFP the process and procedural requirements for security compliance.

- Include security, auditing and logging requirement/description on multi-tenancy model.
- The state will need to provide the security requirements for vendors to respond to and how they will meet the requirements. (Whether the data center is in-sourced or out-sourced.)
- Vendor will need to provide more descriptive information on a solution to address disaster recovery solution based on the state description of DR including resiliency of proposed vendor solution.
- The state needs to provide service expectations for resiliency, possibly as low as the component level.
- Have the vendor describe how they leverage virtual technology to minimize DR costs. Including details on how the solution meets the state RTO/RPO at the lowest cost.

3. What scale of operation would be required for this alternative to be attractive to potential bidders on any future RFP? Is there a critical mass below which you would not be interested in bidding on a proposal for this approach? What metrics would capture that decision?

Operational Review:

- A number of qualitative factors listed by vendors include the RFP approach, scope of the services, alignment with core capabilities, required investment and pricing approach.
- A couple of vendors stated there was no minimum number of virtual instances to make this alternative attractive. The remainder of the responses covered a broad range from as low as 20 virtual instances to 500 virtual instances. With storage size requirements from 20 TB- 30 TB and higher.
- One vendor stated they needed to have a payback starting in 18 months to make this alternative attractive.
- Many vendors stated that limited configurations and high a high degree of standardization would make the opportunity more attractive.

Financial Review:

- Vendors’ responses generally fell into three categories: 1) we sell in a modular or pay-as-you-go arrangement, 2) the scale of a consolidated environment is sufficient to capture economies (one vendor: value optimized when volume > 1,000 virtual machines), and 3) no job too small
- Metrics: number of data centers, unit rates, number of servers virtualized, amount of storage.
- One response suggested that vendors will be hesitant to invest in a technology without a predictable return, and a payback of 18 months or less

Inputs for acquisition:

- Evaluate the potential to hire an industry expert to help the state define the requirements and frame the acquisition. This kind of support should also be available as part of a QA contract.

4. What intellectual property issues, if any, would limit state's ability to pursue this approach? Any proposed solutions must be based on the appropriate technical solution and equipment as opposed to the lead vendor's default proprietary solution.

Operational Review:

- Most responses said this was not an issue. A few said this could be an issue.

Inputs for acquisition:

- This can be covered in more detail in the contracts/legal section of the summary.

5. Given the current decentralized allocation of resources, what role would the transitional data centers in agencies and the statewide data center in Office Building 2 play in your proposed alternative?

Operational Review:

- We do not think the vendors provided value here and believe the vendor had trouble interpreting the question being asked.

Financial Review:

- Documenting application roles and dependencies would be key to understanding roles and/or responsibilities of each party (agency, DIS, contractor).
- Phased transition would allow for application decencies to be understood and managed. May also alleviate concern about remaining useful life of current assets.
- Some vendors point out risk associate with the transition, if governance isn't clearly defined.
- Agency data centers would be a source of subject matter experts (SMEs): "Centralize the operation, keep the experience."
- One vendor noted: "Our approach…does not address the physical move of hardware but rather the smooth transfer of services from the old data center to the new data center."

Inputs for acquisition:

- The state needs to provide better information on the intent of this question.

6. What is a potential timeline for the transitioning of decentralized assets to the data center, equipping of the center, start up of the joint asset, initial operation and training of state employees, and transition of the data center to full state ownership and operation? How would the vendor establish the timeline and what elements would be needed to accurately develop a timeline?

Operational Review:

- Responses about timeline ranged from 6-12 months to 20-41 months. (Vendor estimating 20-41 months sited work with Michigan and Massachusetts). Vendors indicated timing is dependent on the scope of the activity.
- A couple of vendor indicated the legacy systems would have an impact on the timelines.
- Multiple vendors recommend separate engagements to develop answer to the timeline transition question.

Inputs for acquisition:

- The state should develop an approach to the acquisition strategy so the vendors have enough information to provide more detailed timeline.
- Strongly recommend meeting with a select number of vendors who responded to the RFI to gather more information on what they need to provide more detailed response to this question.

7. How would this approach best align or integrate existing legacy systems and mainframe operations with the proposed private cloud for the public sector? How would a vendor handle the continued coexistence of legacy and modernized solutions in transition?

Operational Review:

- Recommended approaches included BizTalk, SOA, rewrite existing mainframe applications to distributed servers.

Financial Review:

- Some vendors indicate willingness to include in scope non-cloud servers and storage. Others tailor the responses to cloud-specific offerings, and assume legacy systems out-of-scope
- Legacy applications and mainframes may be included in scope; some vendors asked the state to reconsider scope.
- As noted by one respondent, “regardless of technology, consistent management of all resources is the goal of the next generation data center.”

Inputs for acquisition:

- Need clarity on what is part of the acquisition at a physical level versus virtual layer such as physical servers for SAP and Mainframe solution.
- Have the vendor describe ways the state can reuse assets and licenses to support the proposed solution.
- The state needs to provide information on the state's role in supporting the legacy system and how state staff work with vendor staff to have these systems work together.
- This is an area that is weak in the responses. The state needs to provide more description on the integration between legacy systems and the vendor responses.
- The state will need to clarify what categories will not be managed by the cloud provider such as agency vendor managed hardware/application (DSHS-PYXIS), physical hardware (DOP-HRMS), mainframes, and systems that are managed by vendors at other locations (DSHS-Provider One).

8. What purchasing and technology decisions might be made now that would limit or enhance the potential for this alternative?

Operational Review:

- Several responses recommended having minimum standards, performance requirements, uptime requirements, and Service Level Agreement for services on the front end.
- One vendor called out consideration for IPv4 and IPv6.
- One of the vendors determined that current acquisitions may not be aligned with the ultimate proposed solution.

Financial Review:

- Delay hardware purchase that would determine or influence the infrastructure platform for cloud computing.
- Begin working on minimum requirements (performance and uptime) and service level agreements.
- Specific recommendation to incorporate backup and recovery environments into scope.
- Applications or software that aren't offered in a virtualized server pricing model may limit extent to which servers can be virtualized.
- Vendor suggests establishing a purchasing governance body, to include agency participation.
- One vendor: "[We] have the ability to integrate with any hardware, software, hypervisor and ITIL based standards."
- One vendor has a specific strategy they call "Leverage Cloud Services."

Inputs for acquisition:

- Include language that calls out the State of Washington IP address space so the state can address the risks and costs to this technology area.
- Include Server Shared Services functional and detailed requirements within the scope of an RFP.

9. What unique financial models might be necessary or advisable to maximize taxpayer value through this alternative deployment strategy?

Operational Review:

- Broad range of pricing with many vendors stating they needed to have a more detailed engagement to provide cost information.
- Many vendors did not detail what is included in the price.
- Multiple responses indicated they would be able to comply with whatever is put forward.

Financial Review:

- Vendors seemed open to: leasing (with variations on payment structure), per-unit pricing, modular pricing, and consulting-only services

Inputs for acquisition:

- Belief is the transformation cost will far exceed the hardware/software cost. We should include language to tease out the cost to support migration and transformation.

RFI ORGANIZATIONAL REVIEW TEAM OBSERVATIONS

In addition to the specific questions in the RFI, the organizational review team identified some important issues that were raised in the responses. They suggest some key issues to consider in any subsequent RFP:

- Update and expand information for vendors that was not in the RFI.
- Include specific requirements relating to contractual items for breech notification.
- Include more detailed information on meeting security investigation, forensics, access, legal hold, and public disclosure.
- Include language that vendor agrees to comply with the state breech notification laws. (Freezing server data logs so they cannot be moving, de-provisioning or re-provisioning when there is a breach, litigation, discovery, etc. The state retains the risk, accountability and responsibility of these items regardless of what type of outsourcing is selected. The vendor needs to provide information on the financial impact to support this.)

- Require that no state data is ever moved, housed or accessed outside of the USA. The vendor agrees to meet the state and federal background check requirements.
- State should include more definition on requirements, particularly desktops.

RFI LEGAL/CONTRACTUAL REVIEW TEAM OBSERVATIONS

The Legal/Contractual group focused only on the potential legal/contractual issues raised in the RFI. It is important to note that this summary is very high level. The legal issues are evolving. The following is a high level synopsis of some issues that may be at issue in the development of the State Data Center (“SDC”) cloud. The list is in no particular order and is not inclusive of every potential area of concern.

Contracting Issues

The Department of Information Services (“DIS”) will need to determine who will be the appropriate parties to the contract, who has strict liability under statute due to role, who has the duty of care for negligence, etc. Without the right parties and contracting vehicles, risk will not be properly allocated.

Prior to releasing the procurement, DIS will need to draft some kind of model terms to provide with the procurement document as required in Information Services Board (“ISB”) standards. The current model contracts are insufficient for this purpose.

Ultimately, the business decision of whether DIS would be liable for all end users will need to be established. If so, how will DIS assure it is passing through relevant contractual obligations and mitigating vicarious liability?

A Service Level Agreement will need to be negotiated as part of the contract with relevant provisions addressing uptime guarantees, maintenance windows, downtime, and the other traditional SLA provisions.

The contract will need to include issues with indemnification, intellectual property indemnification, limitation of liability, representations/warranties, insurance, disclaimers and carve outs. DIS will need to decide its approach to vendor limitation of liability.

With respect to insurance, DIS will need to determine the types of coverage, endorsements, and deductibles appropriate. This will need to be included broadly in the proposed terms let with the procurement.

Due to the constraints set forth below with respect to financing contracts, DIS will need to contemplate structuring the agreement potentially with separate contracts- one for what can be financed, and another for the rest of the engagement. DIS will want to consider both a purchased and personal contract as well, in order to provide the ability if needed to make purchases without consistently filing amendments with OFM. Structuring payment with respect to deliverable, utility rate based, or another form must be considered as well.

Vendor should not be allowed to use previously negotiated agreements with the State due to the large variance in risk and liability associated with the SDC cloud.

What is the “Cloud”?

The National Institute of Standards and Technology (“NIST”) says cloud computing is: "A model for enabling convenient on-demand network access to a shared pool of configurable resources, for example, network servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction."

It needs to be determined what the term “cloud” really means for the SDC:

a. Is it a service provided by a third party, hosted by a third party or hosted by DIS?
b. Is it infrastructure as a service, if so- who owns the equipment?
c. Is it application? If so which?
d. Is it storage capacity?
e. Is it a network of collaboration services that are accessible and are able to be used via the Internet?
f. Is it something else?

The lack of consistency with respect to the undefined term “turnkey” is likely to have resulted in a variety of solutions in the responses. To assure a fair procurement, “cloud computing” should be a defined term to assure all vendors/stakeholders are working from a common understanding. Additionally, DIS should consider whether internal governance and policies are necessary prior to any procurement, or if the Vendor will play a role in the development.

Data.

An internal decision will need to occur with respect to the type of information being pushed into the cloud. A full accounting of the agency/type of data would need to be determined very early to enable an assessment of what regulations apply. Additionally, that information would be useful to enable a vendor to fully price its solution as the regulatory compliance issues would be presented up front. If all of the information in the cloud is publically available, the analysis will be much different than if the information is sensitive and/ or confidential. Will DIS maintain its own services and infrastructure for truly sensitive data?

Agencies may be obliged by virtue of their arrangements with third parties to maintain the secrecy and confidentiality of certain information, so any implemented cloud solution must be able to satisfy those obligations.

Any arrangement would need to assure that the State maintained all ownership in any data in the cloud, as well as the ability to move data to a new service provider without penalty or additional costs.

Data location will be an issue. In the event that DIS acquires equipment, then the data must stay housed on the servers located in the state data center with data backup located in contiguous 48 states as applicable with an auditable guarantee. In the event that DIS acquires a true cloud, then data must remain in the contiguous 48 states with an auditable guarantee. Disaster recovery and data backup roles would need to be established clearly and set forth in a resulting contract.

Will the data be stored in a multi-tenancy environment? If so, what are the guarantees that maintenance, searching, breaches in one sector will not implication the other tenants? It would be important to make sure that the impacts of one tenant’s actions are not felt by the other tenants.

Intellectual Property Issues.

The layers of software and applications involved would require an in-depth approach to IP issue spotting and risk mitigation. To address existing IP issues and mitigate risks of infringement, an inventory and audit of State programs/applications/users must be done and maintained to identify what licenses are at issue. The same should be provided by the Vendor based on its proposal. DIS may wish to consider whether or not to outsource a software license asset manager, as it currently has no system in place to perform this function. Licensing should allow additions of new programs as needed, including known legacy and mainframe systems.

Moreover, potential issues with existing or future use of open source software would need to be identified and addressed. Microsoft licensing typically has a prohibition against open source comingling, so it will be important to understand where potential open source issues may be, as well as what software licenses will be interacting.

The resulting contract should address issues such as ownership of IP created under the contract on behalf of the state. State ownership of work developed under the contract including information architecture of systems/processes such as incident/problem management and Knowledge management of applications. The State should own physical/logical architecture designs, and any/all related documentation. All developed materials and the source code (if applicable) should be retained in escrow, subject to an Escrow Agreement.

Regulatory Compliance.

It will be important for DIS to determine who sets the standards of care for issues such as security and privacy. The arguments would be either DIS since it is DIS data (arguably making DIS liable) or Vendor since vendor has control over the infrastructure. The responsible party will be required to assure all best practices/standards of care are addressed as required by the data in the cloud.

Privacy.

This initial determination of shifting risk will be a necessary step to determining what obligations should be contractually addressed with respect to privacy. Statutory obligations related to notification of breach, as well as damages for breach of privacy should be included in the resulting contract.

Security and Control.

Security is an area that will need to be addressed in more detail. The contract should require the Vendor to establish and auditable security program that demonstrates compliance with ISB security standard compliance and industry best practices. The contract should also address the requirement for at least a SAS-70 audit annually with a copy provided to DIS. Vendors should be prohibited from viewing data without permission, and be required to encrypt data and break into pieces at rest.

Incident Response requirements should be addressed as well, establishing a higher standard of care than the “reasonable person” and requiring due diligence.

Other Regulatory Areas.

Deployment of any solution should keep in mind the issue of out of state access viewed in light of the requirements in the Export Control laws.

Electronic Communications Protection Act.
Depending on the type of data, there would need to be a review of whether that data turned over to a 3rd party would lose its statutory protection under the 4th amendment of the United States Constitution.

Records Retention/ Public Records.
State data must be available for immediate access and removal as needed to comply with records retention requirements for archiving or preservations, as well as compliance with public record laws or potential litigation holds and e-discovery. If multi-tenancy, DIS should consider a requirement that the vendor provide a forensic search tool in order to locate data expeditiously.

Collective Bargaining.
The issue of whether or not any bargaining unit employees are being displaced would need to be addressed early on to determine whether or not the statutory time for notice to the union is required. Additional labor issues may arise as well.

Financing.
Any proposed financing must be done in accordance with statutory requirements and with the requisite authority. For example, if a financing contract is contemplated this must be done through the Treasurer's Office. The financing contract is limited to real /personal property by statute. DIS must be mindful of services, intellectual property, and maintenance.

RFI FINANCIAL REVIEW TEAM OBSERVATIONS

In addition to the specific questions in the RFI, the financial review team identified some important issues that were raised in the responses. They also suggest some key issues to consider in any subsequent RFP:

In general, we see 6 phases in the data center buildout and migration effort:

1. Planning/assessment
2. Design
3. Build
4. Migrate
5. Run/operate
6. Transition back

Scope

- The Team recommends a change in scope to include more than cloud servers. They advise that the final effort should include storage, disaster recovery, network and – perhaps – mainframes and telephony in-scope.
- Integration between technologies is key in the design and build phases. In any case, all systems in and out-of-scope must be integrated

- Need to look to structure of future engagement. The notion of “one throat to choke” is at odds with the reality of what a single vendor can provide. Perhaps a single vendor can act as a general contractor, with subcontractors’ efforts, funding, and payment flowing through.
- Under the “General Contractor” model, consider requiring that the General Contractor also be the Systems Integrator. This would ensure accountability for success of the integration of systems within the project, in addition to the success of the overall span of the project (see diagram below).

Financing

- Financing options: Leasing from vendors is not an option.
- Transforming the costs of this engagement into a lease with the Treasurer seems outside the State Treasurer’s typical approach (COPs typically cover – and are tied to – assets). Perhaps OST might consider a project-financing approach. Pay-as-you-go options may run afoul of OST guidelines, if eventual asset transfer is intended/included in proposals...
- 63-20 financing may also be an option depending on legal and other issues.

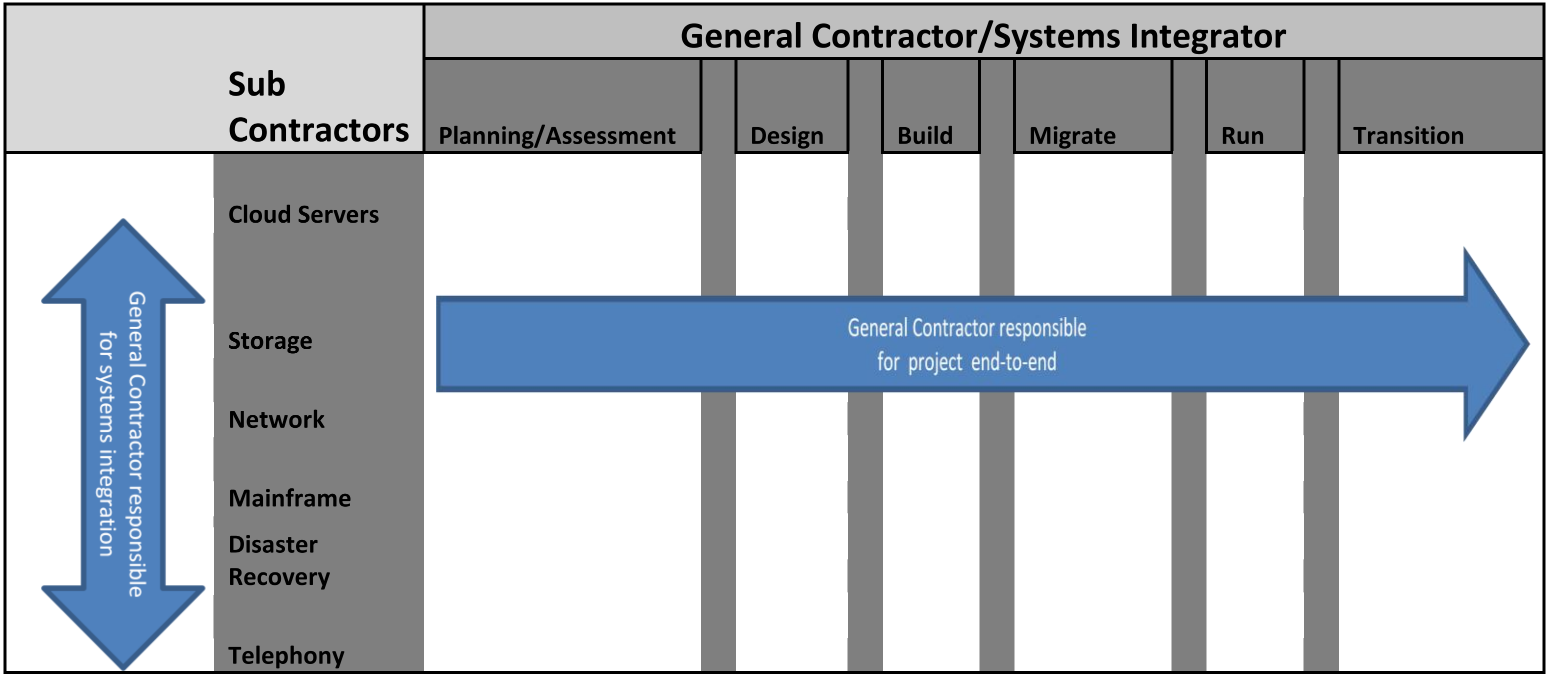
Governance

- Need to establish a QA vendor
- Governance – no guessing about what/who moves
- In the interim, purchases should not be made that define/constrain/interfere with a future infrastructure platform

Other Considerations

- We need to consider the impact of automation, as it relates to support staffing in the “Run/Operate” phase. Establishment and tracking of support metrics would be required at this phase
- How do we determine term of the engagement? Asset life?
- Marketing to new customers within the bounds of authorizing legislation…how can this be worked into an RFP?

Diagram of “General Contractor” model


General Contractor/Systems Integrator
Sub Contractors
Planning/Assessment
Design
Build
Migrate
Run
Transition
Cloud Servers
Storage
Network
Mainframe
Disaster Recovery
Telephony
General Contractor responsible for systems integration
General Contractor responsible for project end-to-end